UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/763,814	01/22/2004	Anthony F. Gigliotti	035813-003	5015

46188 7590 03/15/2010

Nixon Peabody LLP
P.O. Box 60610
Palo Alto, CA 94306

EXAMINER	
VO, TED T	
ART UNIT	PAPER NUMBER
2191	
MAIL DATE	DELIVERY MODE
03/15/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/763,814
Filing Date: January 22, 2004
Appellant(s): GIGLIOTTI ET AL.

John P. Schaub
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 12/18/2009 appealing from the Office action mailed 10/01/2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is incorrect. A correct statement of the status of the claims is as follows:

Claims 1-15 and 20-36 have been non-Final rejected.

Claims 16-19 are canceled.

Claims 1-15 and 20-36 are on appeal.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments ~~after final rejection~~ contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows:

"Claims 1-15, 20-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Microsoft White Paper, "Understanding Patch and Update Management: Microsoft's Software

Update Strategy", Microsoft Corporation, pages: i-iii, 1-14, October 2003, and in further view of Microsoft computer dictionary (or a peer-to-peer network architecture definition), submitted in IDS as "Microsoft Corporation, "peer-to-peer architecture", Microsoft Computer Dictionary, Fifth Edition (2002), p. 397".

The correction is necessary because Examiner has the typo error.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Microsoft White Paper, "Understanding Patch and Update Management: Microsoft's Software Update Strategy", Microsoft Corporation (October 2003), pp. i-iii, 1-14

Microsoft Corporation, "peer-to-peer architecture", Microsoft Computer Dictionary, Fifth Edition (2002), p. 397

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Based on the Appellants' arguments of the claims on appeal, the claims will be rearranged in groups as follows:

As per claims 1, 20, 35 and 36: Claim 1 is controlled claim. Regarding the limitation of claim 1, Microsoft white paper discloses: ***A method for automatically distributing a software update to a network [****of devices of a peer-to-peer network****] controlled by an organization, the method comprising:***

receiving application and system information from one or more inoculation clients installed on the devices, the receiving performed via [*peer-to-peer****] communication***

(See p.4, paragraph:

- The Security Bulletin Notification Service enables customers to receive timely and accurate information directly from Microsoft about worms, viruses, and other security events. It represents one of the first steps taken to help customers determine if an event is relevant to their environments, how and when to download and deploy the security patches, and how the software updates or security patches affect their overall IT infrastructures. **Customers can sign up to be notified via e-mail when the latest Security Bulletins are posted with versions for business IT professionals and end users**.

And further see, p. 9: first bullet:

- The **Office Update Inventory Tool v1.5** enables administrators to check one or more computers for the status of Office 2000 and Office XP updates. Administrators can run the tool from one central location to check the status of all computers in their organizations. The tool produces a report used to determine which updates have been applied, which updates are available to be applied, and which updates can be applied only to an administrative image.),

comparing the application and system information with application and version information in *[a global]* ***update repository to determine if an update exists for a corresponding application controlled by an inoculation client,*** *[the global update repository including updates from multiple application manufacturers];*

(See p. 9, paragraph within first bullet:

- The **Office Update Inventory Tool v1.5** enables administrators to check one or more computers for the status of Office 2000 and Office XP updates. **Administrators can run the tool from one central location to check the status of all computers in their organizations**. The tool produces a report used to determine which updates have been applied, which updates are available to be applied, and which updates can be applied only to an administrative image.

And see all p. 11, paragraph 3 within 'Office Update Inventory Tool':

3. Office Update Sync Tool is deployed by the Installer and runs on a single computer that has an Internet connection. It periodically checks the **Microsoft downloads Web site to download the latest Office Update Inventory Tool and Office Update Inventory Database**. It then uses SMS distribution points within the SMS infrastructure to send the latest versions of these items to client computers.

queueing the update if an update exists for an application controlled by an inoculation client;

receiving a communication from the corresponding inoculation client checking for available distribution jobs;

(See Microsoft Baseline Security Analyzer V1.1.1 or MBSA v1.1.1 (p. 7-8). It has a command line interface with a scheduling tool "Task Scheduler". (Examiner takes note: Since "queuing" has the means of lining up; a task scheduler does queuing). Further see p. 11, within "Security Update Inventory Installer" see item 3;

> 3. Security Update Sync Tool is deployed by the Installer and runs on a single computer that has an Internet connection. **It periodically checks the Microsoft downloads Web site to download the latest security update bulletin catalog**. It then uses SMS distribution points within the SMS infrastructure to send the latest versions of these items to client computers.

and within "Office Update Inventory Tool", see item 3.

> 3. Office Update Sync Tool is deployed by the Installer and runs on a single computer that has an Internet connection. **It periodically checks the Microsoft downloads Web site to download the latest Office Update Inventory Tool and Office Update Inventory Database. It then uses SMS distribution points within the SMS infrastructure to send the latest versions of these items to client computers.**); ***and***

automatically transmitting the update to the corresponding inoculation client in response to the receiving a communication if an update exists for an application controlled by the corresponding inoculation client (See Distribute Software Updates Wizard Installer (p. 11-12) and see Office Update Inventory Tool. Furthermore, see p. 11, within "Security Update Inventory Installer", item 3; and within "Office Update Inventory Tool", item 3. 'It then uses

SMS distribution points within SMS infrastructure to send the latest version …", and see whole section within p. 11-12: "Distribute Software Updates Wizard Installer").

Microsoft does not explicitly mention to receive information from "peer-to-peer" , but a network. However, The Microsoft computer dictionary defines the data distribution via peer-to-peer: See peer-to-peer architecture, p. 397. It appears that any computers which are communicable in a network can share data, thus can be modified as peer computer. The adding of peer-to-peer network is only changing in shape, but does not provide any new or unexpected result in term of receiving a patch.

Therefore, it is obvious to an ordinary in the art to use either client/server architecture or being combined with a peer-to-peer architecture as defined in the Microsoft computer dictionary because it would yield predictable result.

Furthermore, Microsoft does not explicitly mention GLOBAL UPDATE REPOSITORY, that includes updates from multiple application manufacturers.

However, the Microsoft Download websites (see Hyperlinks) and see p. 13, paragraph in first bullet "Microsoft Update", there is a mention of a centralized storage to either a SQL database or Network share. These sites are repository that can store any types of data.

Therefore, it would be obvious to the ordinary in the art that the download websites (hyperlinks) and centralized storage could store any data (i.e. multiple application manufacturers). If data is permissible for use in a global update repository it would ease patching management.

As per Claims 2-8, 12, 14-15: Appellants summit no arguments on claims 2-8, 12, 14-18, Therefore, the claims have the same rejection as of the controlled claim 1.

As per Claim 9: Regard claimed limitation, *The method of claim 8, therein the global update repository mines, retrieves, and archives external update information.*

Claim 9 further recites "*global update repository mines, retrieves, and archives external update information".*

Claim 9 recites further limitation of "*global update repository*" which mines, retrieves and archives external update information. As noted from the rejection of claim 1, Microsoft does not explicitly mention "*global update repository*". However, it is obvious to an ordinary in the art when viewing the update websites or the centralized storage, SQL database, or network share to include the extra features. Mining, retrieving, and to achieving are the functions of a storage server. The use of "*global update repository*" is another name of the storage server. Microsoft white paper shows a Security Update Service (SUS) server, acting like *global update repository* (see p. 9-10, section "Software Update Service"; particularly, see four consecutive paragraphs, the started paragraph "For example.." in p. 10). The SUS server can store, retrieve patches and update information from external update information. Furthermore, mining, retrieving, achieving information are the functions of a storage server. Microsoft white paper mentions the SQL database, network share. These are storage servers and thus are known for miming, retrieving and achieving update information (see p. 13, Microsoft white paper mentions centralize storage, SQL database, network share). Therefore, it is obvious to the ordinary in the

art to include mining, retrieving, achieving external update information, because mining, retrieving, and archiving data/information are the functions of storage servers.

As per Claim 10: Regarding the limitation, *The method of claim 9, wherein the external update information is mined and retrieved from external security websites.*

Claim 10 recites further limitation of "*global update repository*" where it further functionalized as that *the external update information is mined and retrieved from external security websites.*

See the same rejection as of claim 9, where SUS server is Security Update Service server.

As per Claim 11: Regarding the limitation, *The method of claim 10, wherein the global update repository uses web spiders*

Claim 11 recites further limitation of "*global update repository*" where it further functionalized as that *uses web spiders.*

As noted from the rejection of claim 1, Microsoft does not explicitly mention "*global update repository*". However, the update websites or the centralized storage, SQL database, or network share to include search mechanism that consolidate with location customers to help searching for patches (see p. 4, "Security Bulletin Web search tool"). It should be noted that "spider web" is another name of a search engine, which is known in the art. Search engine is usually put in a webpage of a web site. Microsoft web sites and centralized storage as cited are operated similarly with "search tools" (*web spider*). See p. 13, second bullet, a centralized storage, SQL database). Therefore, it is obvious to an ordinary in the art when viewing search tools would direct to the web spider, since being included with "web spider" is only the name different from the prior art and it produces no new or unexpected result.

As per Claim 13: Regarding limitation, *The method of claim 9, wherein the external update information contains a vendor type, the vendor type being automatic download and release, automatic download and manually confirm release, or manually download and confirm.*

Claim 13 further recite *global update repository archives external update information* which contains a vendor type which allows either automatic download or manual download with confirm. As noted, Microsoft does not explicitly mention "*global update repository*". However, it is obvious to an ordinary in the art when viewing the update websites or the centralized storage, SQL database, or network share. These servers are storage severs which are available for storing any types of data, including vendor types. It allows a user to click on the links to download data. The websites (See hyperlinks, e.g. hyperlinks in p. 14) suggest the data is stored in these sites as update information; which might be from Microsoft's products or of Microsoft's vendors who are the partners (see p. 10, see three consecutive paragraphs, the started paragraph "For example..", and refer to p. 13, second bullet, a centralized storage, SQL database).

As per claim 20-34: Appellants form claim 20-34 as a group. Appellants provide no specific arguments. Claim 20 of this group is grouped in the group of claim 1 above. Therefore, claims 20-34 have the same rejection according to the controlled claim 1.

(10) Response to Argument

A. Appellants submit arguments on Claims 1, 20, 35, and 36 as a Group.

-A1. Appellants argue Microsoft white paper does not disclose: *"[r]eceiving application and system information from one or more inoculation clients installed on the devices"* (Brief: p. 13)

-A2. Appellants argue the Examiner statement "In further view of Microsoft Dictionary" does not provide the cited reference in the record (Brief: p. 14).

-A3. Appellants argue the obviousness in combining the Microsoft's white paper and the definition of peer-to-peer is based on hindsight reasoning. In brief, p. 14, Appellants depict the Examiner's argument where Appellants take the tense "is" used in Examiner's office action to indicate the Examiner's conclusion of obviousness is based on hindsight reasoning; i.e. the obviousness is based upon knowledge as of the date of the office action.

(Brief: p. 14:

"[A]dditionally, the Examiner's statement "It should be noted that a distribution of a piece of software or of patches in a network is not new in the art. It is done commonly in software companies whose clients are frequently attacked by hackers."[3] indicates the Examiner's conclusion of obviousness is based on improper hindsight reasoning. In more detail, the Examiner's use of the verb "is," which is the present tense form of the verb "to be" indicates the Examiner's conclusion of obviousness is based upon knowledge as of the date of the Office Action, which is after the time the claimed invention was made.")

-A4. Appellants submit Microsoft white paper refers a global update repository for a single vendor's products; it does not disclose a global update repository that includes update from multiple application manufacturers (Brief: p. 15-16) .

-A5. Appellants submit Microsoft white paper in view of Microsoft computer dictionary does not disclose comparing as of claim 1 (Brief: p. 15).

B. Appellants submit arguments on Claims 9, 10, 11, 13.

- With regard to claim 9, Appellants submit Microsoft does not disclose *global update repository mines, retrieves, and archives external update information;* Appellants submit Microsoft says nothing about the recited limitation.

- With regard to claim 10, Appellants submit Microsoft does not disclose *the external update information is mined and retrieved from external security websites.* Appellants submit Microsoft says nothing about the recited limitation.

- With regard to claim 11, Appellants submit Microsoft does not disclose *global update repository uses web spiders.* Appellants submit Microsoft says nothing about the recited limitation.

- With regard to claim 13, Appellants submit Microsoft does not disclose *the external update information contains a vendor type, the vendor type being automatic download and release, automatic download and manually confirm release, or manually download and confirm.* Appellants submit Microsoft says nothing about the recited limitation.

C. Appellants submit arguments on Claims 20-34 as a group, and Appellants submit the claims 20-34 are means-plus-functions, Appellants submit the rejection of claim 20-34 cannot be drawn as in the same rejection of claim 1-15.

Examiner's response to the arguments:

A. Appellants submit arguments on Claims 1, 20, 35, and 36 as a Group.

A1. Appellant argues Microsoft white paper does not disclose: "*[r]eceiving application and system information from one or more inoculation clients installed on the devices*".

Examiner respectfully disagrees: Based on the generic and broad recitation, Examiner finds that the reference alone or in combination addresses the recitation.

In light of the specification, it generally describes applying patches in a computer in a corporate network. It has system administrator, corporate network (spec: [0007]) and clients/ servers within the corporate, and centralized repository, and an inventory control engine to determine comparing for update (spec:[0026]). The specification does not describe clearly the functions of the steps recited in the claims. For example, Appellants' recitation "*[r]eceiving application and system information from one or more inoculation clients installed on the devices*" merely repeats the specification of block 604 in FIG. 6.

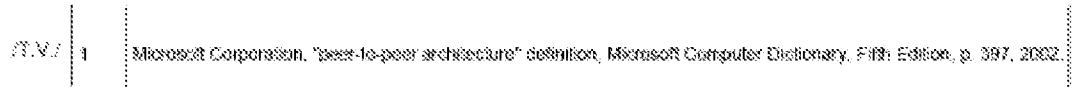
Lack of details in the specification, Examiner takes an interpretation of "*receiving application and system information*" as the information being downloaded or being available

viewed in a computer via network. For example, when a user views a webpage, simply, the information in the webpage is the remote data from a website which is downloaded to the user computer. Therefore, "receiving" in light of the specification means data from another computer and it is available in a computer. Microsoft white paper provides Window update connecting between two separated computers, where the information of computer's operating system, software, and hardware is provided in a site and viewable from another site. For example, in "Window Update" (P.7, Para: "Window Update"), it is an online operation; see "[N]ew content is added to the site regularly providing the most recent updates and fixes to protect computers". Microsoft white paper also provides Office Update (p.7-8: section "Office Update") which is similarly to Window Update, where the application such Office 2000, or Office XP, and computer information of a user will be analyzed remotely by an administration for its service update (p. 8: see bullet: 'Administrators can run the tool from one central location to check the status of all computers in their organizations. The tool produces a report used to determine which updates have been applied, which updates are available to be applied, and which updates can be applied only to an administrative image').

With the discussions in the Microsoft white paper and the websites shown as the hyperlinks (e.g. see p. 14), it discloses the recitation "receiving application and system information performed via network communications". It should be noted that Microsoft white paper does not mention "peer-to-peer", but the combination with the definition of "peer-to-peer architecture" in the Microsoft computer dictionary would be necessary and obvious under 35 USC 103(a).

A2. Appellants argued the Examiner statement "In further view of Microsoft Dictionary" does not provide the cited reference in the record (Brief: p. 13).

Examiner respectfully answers: It is only typo error. Examiner typed the words "Microsoft dictionary" is a typo error, but it is clearly directed to the reference of record which is submitted by Appellant in the IDS filed on 07/07/2008, considered by Examiner as:



In the office action, this reference has been cited to p. 397. It appears being a typo error.

A3. Appellants argue the obviousness in combining the Microsoft white paper and the definition of peer-to-peer is based on hindsight reasoning. In brief, p. 14, Appellants depict the Examiner's argument where Appellants take the tense "is" used in Examiner's office action to indicate the Examiner's conclusion of obviousness is based on hindsight reasoning; i.e. the obviousness is based upon knowledge as of the date of the office action (Brief: p. 14)

Examiner respectfully disagrees: The argument in the office action aims to show that the word "peer-to-peer" is known in the art; at least it is based on the published date of the Microsoft computer dictionary. Being included with 'peer-to-peer" in the claims, it is only the name difference. It yields predictable result. It would be obvious to combine the patch management discussed in the Microsoft white paper with the definition of "peer-to-peer architecture". Thus, it would be obvious to an ordinary in the art to include the peer-to-peer architecture when viewing the definition of "peer-to-peer architecture" in term of patching. Microsoft white paper suggests that patching is for preventing "hacking" (see p.1, Introduction), "worm" or "virus" attacks (See p. 5, table 1). The use of tense made by the Examiner could be wrong, but the fact is that it is

suggested or disclosed from Microsoft white paper, a prior of record in term of "virus", "worm" and "hacker". Therefore, merely referring to the tense "is" used in Examiner's argument to indicate the obviousness which is concluded based on hindsight reasoning and upon knowledge as of the date of the office action is improper.

Moreover, in further response to this argument, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

A4. Appellants submit that Microsoft white paper refers a global update repository for a single vendor's products; it does not disclose a global update repository that includes update from multiple application manufacturers.

Examiner respectfully responds:

Examiner submits that Microsoft white paper does not explicitly mention "Global Update Repository". However, it is obvious in viewing of various Microsoft download websites (See p. 7, sec. For Users and Small Organizations", see downloaded websites on hyperlinks) and the mentioning of "centralized storage", "SQL database", "network share" (p. 13, second bullet). All these websites of Microsoft are available through Internet (e.g. see Introduction, p. 1); they are the storage servers. A server is a computer which is linked to network; its storage is available for storing any types of data which can be retrieved or downloaded via a hyperlink.

Appellants alleged that the Microsoft download websites to which Examiner refers are only to single vendor's products; it is Microsoft products. Examiner respectfully disagrees. The Appellants' statement is only based on generic allegations.

First of all, the claims "multiple manufactures" appears contradicting to the preamble, because the preamble recites updating for a "**single product**". See it recites: ***A method for automatically distributing a software update*** (Preamble); see "**the application**" (in the claims' body). Thus, using single software in the preamble and making single software with "multiple manufactories" causes the claim inconsistent.

Secondly, the term Global Update Repository is interpretable; it is nothing but one or more storage servers on Internet. Therefore, if this location includes multiple products, the recitation is unnecessary because the term "the application" in the claims meets only "one product". For this, it reads on either a generic vendor's product including the product from Microsoft which is available from a Microsoft website (see the hyperlinks in p. 14). Thus, even including "multiple products", the software update recited in the claims remains updating one application or a single software update ("the application" as recited).

Thirdly, it should be noted that the recitation is addressed under the obviousness under 35 USC 103(a). Microsoft does not use exactly the claimed terms, however, its servers are **the repositories** (refer to "centralized storage", "network share"). The claim refers to "repository" which is the term of storage. A storage is known in computing for storing data. A storage server can store any types of data if permissible (under copy right protection). Like our computer, the computer can store various software products of different manufactories. Thus the centralized storage ('network share') of Microsoft might include its partner's software such as of IBM, SUN,

or of its vendors, or whatever products stored and available for being downloaded from the Microsoft websites. Examiner has addressed a storage is obvious as being available for storing any types of information under 35 USC 103(a.

A5. Appellants submit Microsoft white paper in view of Microsoft computer dictionary does not disclose comparing as of claim 1.

Examiner respectfully disagrees: Based on the generic and broad recitation, Examiner finds that the reference alone or in combination addresses the recitation.

As provided in the summary of the claim 1 in the Appeal brief (Appellants refer as: FIG. 6, reference numeral 608 and para. [0026] lines 14-18), it generally describes comparing as a determination if an update is existed using an "inventory control engine".

See the specification, para. [0026]:

> "[A]t 606, the application and system information may be compared with application and version information in the global update repository to determine if an update exists for a corresponding application controlled by an inoculation client. This may include utilizing an HTTP GET or POST command and may be performed by **an inventory control engine**." (emphasis added).

Examiner has submitted that Microsoft white paper in view of "peer-to-peer architecture" (the Appellants' IDS) discloses comparing (See p. 4: The **Office Update Inventory Tool v1.5** enables administrators to check one or more computers for the status of Office 2000 and Office XP updates. Administrators can run the tool from one central location to check the status of all computers in their organizations. The tool produces a report used to determine which updates have been applied, which updates are available to be applied, and which updates can be applied only to an administrative image. See p. 7, Windows update and Microsoft Baseline Security Analyzer V1.1.1; see p. 8 and p. 9, Office update; see p. 10: Security Update Sync Tool is deployed by the Installer and runs on a single

computer that has an Internet connection. It periodically checks the Microsoft downloads Web site to download the latest security update bulletin catalog).

It should be noted that comparing is used in every software update. Microsoft white paper provides the update inventory tool and security update sync tool to perform patch management. The tools will produce the reports to determine which updates have been applied. The tools determine which computer requires patch management (see Office Update Inventory Tool v1.5 and Microsoft Baseline Security Analyzer V1.1.1). Without knowing the statuses of software and computers information, the update cannot be performed. This is the basis of software update. This reads on comparing the application and system information with application and version information.

B. Appellants submit arguments on Claims 9, 10, 11, 13, where Appellants submits Microsoft white paper says nothing about the recitations in the claims 9, 10, 11, and 13.

Examiner respectfully disagrees to the arguments as specified in claim 9, 10, 11, and 13.

It should be noted that claims 9, 10, 11, 13 are dependent on claim 1. Each of the claims recites the extra feature of the limitation "Global update repository". Base on the recitation "distributing a software update" and "the application" recited in claim 1, the update of the claim is referred to one application in "Global update repository". Thus, the extra features in claims 9, 10, 11, 13 contribute no functions to the method claim 1, but act like adding ingredient without yielding any new result to the "application" which is used for update. Such adding contributes cosmetic to the "Global update repository" and it is obvious under 35 USC 103(3).

In the rejection, Examiner has submitted Microsoft white paper does not mention "Global update repository". Microsoft white paper shows the updating web sites and a centralized storage, network share. Any of these sites is obvious to be or to be modified into a repository in which it is claimed as "Global update repository". In the discussions of the Microsoft white paper, it has a Software Update Services (SUS) server that can store and deploy patches (p. 10, three first consecutive paragraphs). It has search tools (see p. 4, Security Bulletin Web search tool: 'web spider'), it has hyperlinks to retrieve update information, and it provides storage for achieving information (p. 13: centralized storage/network share: 'archive external information'). The storage servers/repositories can obviously provide the non-related features as recited in the claims 9, 10, 11, 13.

> Ex parte Rubin , 128 USPQ 440 (Bd. App. 1959) (Prior art reference disclosing a process of making a laminated sheet wherein a base sheet is first coated with a metallic film and thereafter impregnated with a thermosetting material was held to render prima facie obvious claims directed to a process of making a laminated sheet by reversing the order of the prior art process steps.). See also In re Burhans, 154 F.2d 690, 69 USPQ 330 (CCPA 1946) (**selection of any order of performing process steps is prima facie obvious in the absence of new or unexpected results**); In re Gibson, 39 F.2d 975, 5 USPQ 230 (CCPA 1930) (Selection of any order of mixing ingredients is prima facie obvious.).

C. Appellants submit the arguments on Claims 20-34 as a Group, and Appellants submit the claims 20-34 as they are means-plus-functions. Appellants submit that the rejection of claims 20-34 cannot be drawn as in the same rejection of claims 1-15.

Examiner respectfully disagrees: The claims 20-34 are the apparatus claims. The claims have the functionality corresponding to the recited limitations in the method of claims 1-15.

Since Appellants submit the claims 20-34 are in a group, where the leading claim 20 appears being an apparatus which has the functionality corresponding to the limitations in claim 1 and claim 20 was named in the group of claim 1, claims 20-34 should stand or fall together with claim 1.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

TTV
March 11, 2010

/Ted T. Vo/
Primary Examiner, Art Unit 2191

Conferees:

Wei Y. Zhen, SPE.
/Wei Y Zhen/
Supervisory Patent Examiner, Art Unit 2191

Lewis A. Bullock, SPE.
/Lewis A. Bullock, Jr./
Supervisory Patent Examiner, Art Unit 2193